Begrijp het Protocol van de Resolutie van het Adres van de Volmacht (ARP)

Inhoud

Inleiding

Dit document beschrijft hoe Proxy ARP machines op een subnetnetwerk helpt om externe subnetten te bereiken zonder de noodzaak om routing of een standaardgateway te configureren.

Voorwaarden

Vereisten

Dit document vereist een goed begrip van het Proxy Address Resolution Protocol (ARP) en de Ethernet-omgeving.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®softwarerelease 12.2(10b)
- Cisco 2500 Series routers

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

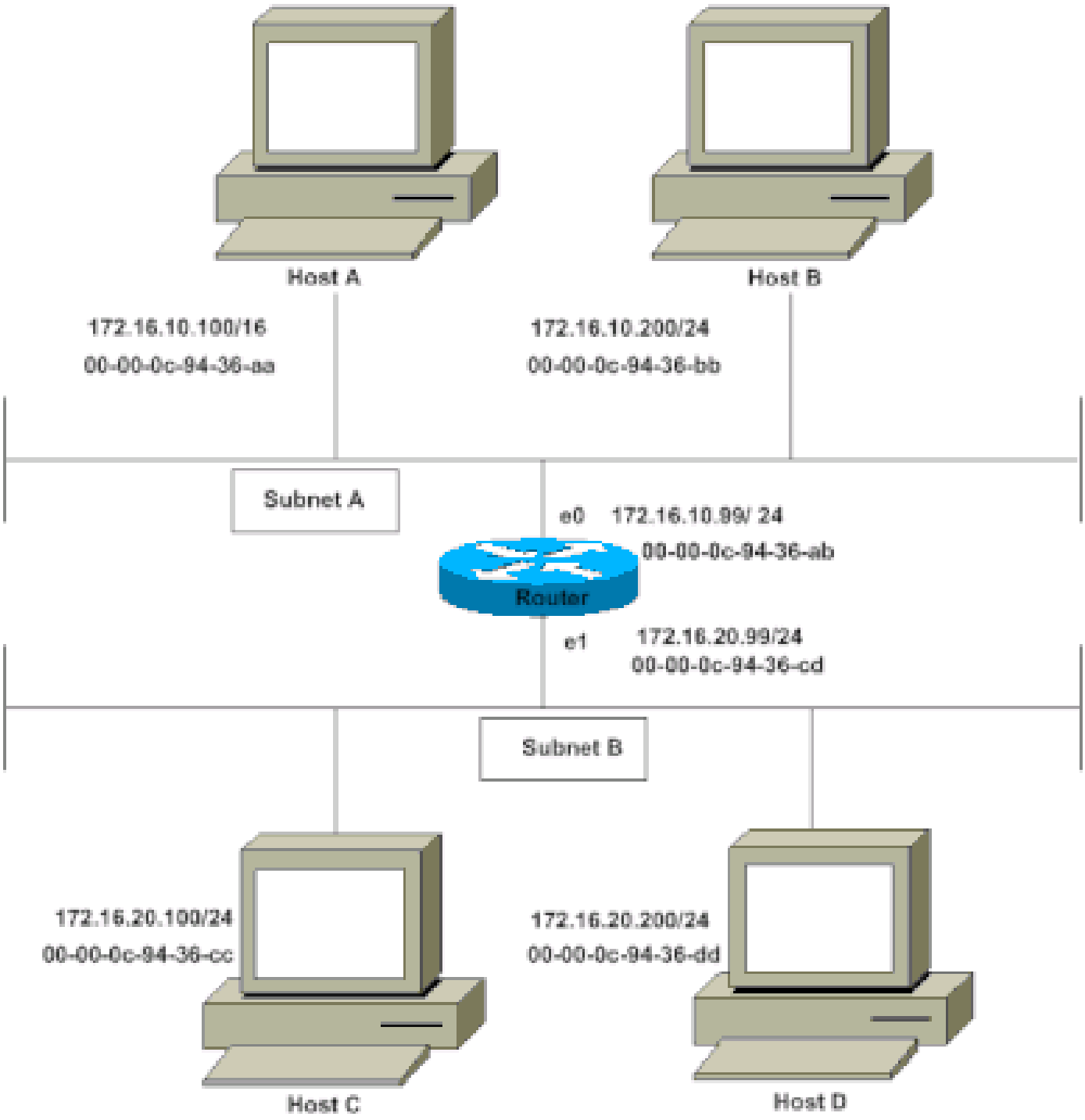
Achtergrondinformatie

In dit document wordt het begrip proxy Address Resolution Protocol (ARP) uitgelegd. Proxy ARP is de techniek waarin één host, meestal een router, ARP-verzoeken beantwoordt die bedoeld zijn voor een andere machine. Als u zijn identiteit vervalst, neemt de router de verantwoordelijkheid op zich voor het routeren van pakketten naar de "echte" bestemming. Proxy ARP kan machines op een subnetnetwerk op afstand te bereiken zonder de noodzaak om routing of een standaardgateway te configureren. Proxy ARP is gedefinieerd in RFC 1027 .

Hoe werkt proxy-ARP?

Dit is een voorbeeld van hoe proxy ARP werkt:

Netwerkdiagram



Netwerkdiagram

De host A (172.16.10.100) op Subnet A moet pakketten verzenden naar host D (172.16.20.200) op Subnet B. Zoals in het diagram wordt getoond, heeft Host A een /16 subnetmasker. Wat dit betekent is dat Host A gelooft dat het direct verbonden is met het hele netwerk 172.16.0.0. Wanneer host A moet communiceren met alle apparaten waarvan het denkt dat ze direct verbonden zijn, stuurt het een ARP-verzoek naar de bestemming. Daarom wanneer Host A een pakket naar Host D moet verzenden, is Host A ervan overtuigd dat Host D direct verbonden is, zodat het een ARP-verzoek naar Host D.

Om Host D (172.16.20.200) te bereiken, heeft Host A het MAC-adres van Host D. nodig.

Daarom zendt Host A een ARP-verzoek uit op Subnet A, zoals wordt getoond:

MAC-adres afzender	IP-adres van afzender	MAC-adres doel	Doel IP-adres
00-00-0c-94-36-a	172.16.10.100	00-00-00-00-00-00	172.16.20.200

In dit ARP verzoek, host A (172.16.10.100) vraagt dat host D (172.16.20.200) zijn MAC-adres verzenden. Het ARP-verzoekpakket wordt vervolgens ingekapseld in een Ethernet-frame met het MAC-adres van host A als bronadres en een broadcast (FFFF.FFFF) als doeladres. Aangezien het ARP verzoek een uitzending is, bereikt het alle knooppunten in Subnet A, dat de e0 interface van de router omvat, maar bereikt geen Host D. De uitzending bereikt geen Host D omdat de routers, door gebrek, geen uitzendingen door:sturen.

Aangezien de router weet dat het doeladres (172.16.20.200) op een andere subnetverbinding staat en Host D kan bereiken, antwoordt het met zijn eigen MAC-adres aan Host A.

MAC-adres afzender	IP-adres van afzender	MAC-adres doel	Doel IP-adres
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-a	172.16.10.100

Dit is het Proxy ARP-antwoord dat de router naar host A verstuurt. Het proxy ARP antwoordpakket is ingekapseld in een Ethernet-frame met MAC-adres van de router als bronadres en het MAC-adres van host A als doeladres. De ARP-antwoorden zijn altijd unicast op de oorspronkelijke aanvrager.

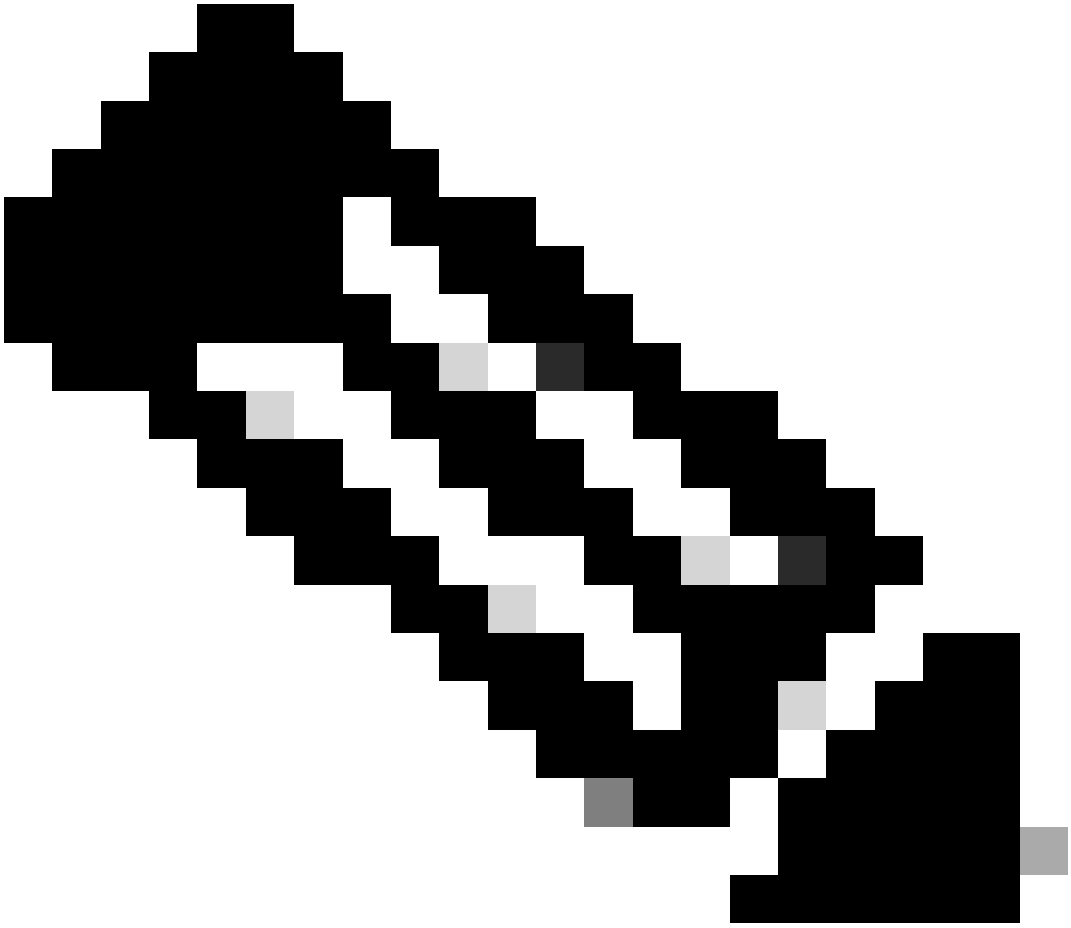
Na ontvangst van dit ARP antwoord, host A werkt zijn ARP tabel bij, zoals getoond:

IP-adres	MAC-adres
172.16.20.200	00-00-0c-94-36-ab

Vanaf nu, host A doorstuurt alle pakketten die het wil bereiken 172.16.20.200 (host D) naar het MAC-adres 00-00-0c-94-36-ab (router). Aangezien de router weet hoe te om Host D te bereiken, door:sturen de router het pakket aan Host D. Het ARP-cache op de hosts in Subnet A wordt gevuld met het MAC-adres van de router voor alle hosts op Subnet B. Daarom worden alle pakketten die zijn bestemd voor Subnet B naar de router verzonden. De router stuurt die pakketten door naar de hosts in Subnet B.

Het ARP-cachegeheugen van host A wordt in deze tabel weergegeven:

IP-adres	MAC-adres
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.99	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb



Opmerking: meerdere IP-adressen zijn toegewezen aan één MAC-adres, het MAC-adres van deze router, wat aangeeft dat proxy ARP in gebruik is.

De interface van Cisco moet worden geconfigureerd om proxy-ARP te accepteren en erop te reageren. Dit is standaard ingeschakeld. Het **no ip proxy-arp**bevel moet op de interface van de router worden gevormd die aan de ISP router wordt aangesloten. Proxy ARP kan op elke interface afzonderlijk worden uitgeschakeld met de opdracht voor interfaceconfiguratie **no ip proxy-arp** , zoals wordt getoond:

<#root>

```
Router#
```

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

```
 interface ethernet 0
```

```
Router(config-if)#
```

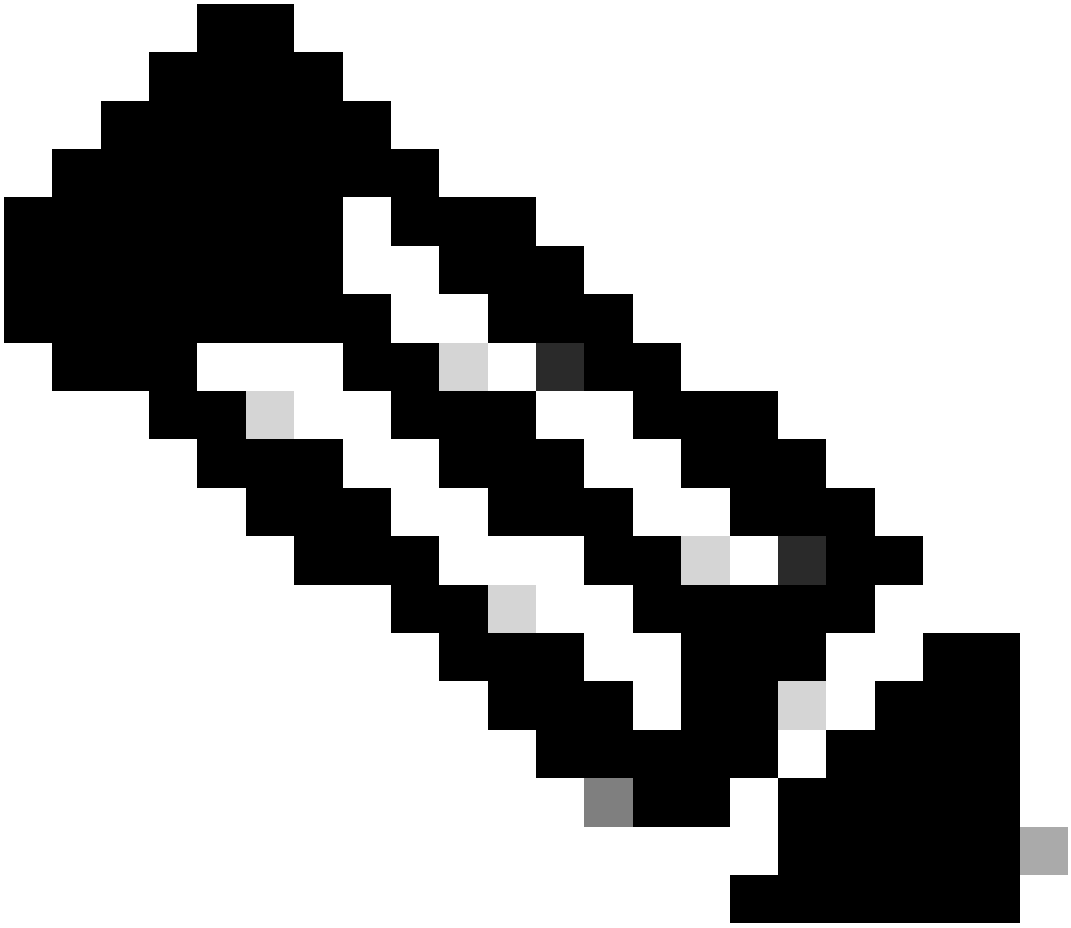
```
 no ip proxy-arp
```

```
Router(config-if)#
```

```
^Z
```

```
Router#
```

Om volmacht ARP op een interface toe te laten, geef het bevel van de **ip proxy-arp**interfaceconfiguratie uit.



Opmerking: wanneer Host B (172.16.10.200/24) op Subnet A probeert pakketten te verzenden naar bestemmings-Host D (172.16.20.200) op Subnet B, kijkt het in zijn IP-routeringstabel en routeert het pakket dienovereenkomstig. Host B (172.16.10.200/24) heeft geen ARP voor Host D IP-adres 172.16.20.200 omdat het tot een ander subnetnummer behoort dan wat op Host B Ethernet-interface 172.16.20.200/24 is geconfigureerd.

Voordelen van Proxy ARP

Het belangrijkste voordeel van volmacht ARP is dat het aan één enkele router op een netwerk kan worden toegevoegd en de routeringstabellen van de andere routers op het netwerk niet verstoort.

Proxy ARP moet worden gebruikt op het netwerk waar IP-hosts niet zijn geconfigureerd met een standaardgateway of geen routerintelligentie hebben.

Nadelen van proxy-ARP

De gastheren hebben geen idee van de fysieke details van hun netwerk en veronderstellen het om een vlak netwerk te zijn waarin zij om het even welke bestemming kunnen bereiken als zij een ARP verzoek verzenden. Wanneer je ARP voor alles gebruikt zijn er nadelen. Dit zijn enkele van de nadelen:

- Het verhoogt de hoeveelheid ARP verkeer op uw segment.
- Hosts hebben grotere ARP-tabellen nodig om IP-naar-MAC-adrestoewijzingen te kunnen verwerken.
- De beveiliging kan worden ondermijnd. Een machine kan beweren een andere te zijn om pakketten te onderscheppen, een daad genaamd "spoofing."
- Het werkt niet voor netwerken die geen ARP gebruiken voor adresresolutie.
- Het generaliseert niet naar alle netwerktopologieën. Bijvoorbeeld, meer dan één router die twee fysieke netwerken verbindt.

Gerelateerde informatie

- **IP-ondersteuningsresources**
- **Ondersteuningspagina voor NAT**
- **Tools en bronnen**
- **Cisco Technical Support en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.